Policy Monitor

Service Definition

Overview

Cyber Security Policy Monitor (CSPM) is a web-based cyber security framework designed to help SMEs achieve compliance of the most prestigious security standards available. This G-Cloud service helps you navigate the pain-staking process of configuring their security policies and applying for certification by applying ease-of-use 'tasks' which you can assign to different members of your organisation. The solution provides users who do not have the resources for employing a Chief Information Security Office (CISO) and their team, access to information on cyber security sufficient to enable small organisations to gain an understating of cyber security issues, to complete the first simple steps in cyber security and to then identify people and organisations who can then help them to move from the basic to a relevant form of cyber security accreditation.

Information Assurance

CSPM is not an accredited solution as regards specific information assurance ¨C Impact Levels (IL).

Backup Restore and Recovery

Backup of the database is performed daily. The testing of recovery is performed regularly. This back up is of the entire database as a whole and it is a protection against data corruption of the environment. As the solution is a multi-tenanted platform containing data of multiple organisations, it is not possible to provide an individual restore of a single organisation's data in the event of error.

It would be possible as a costed server to go back to a historic backup, extract and re-load that data.

On Boarding and Off Boarding

On boarding is a straightforward process. A system administrator enters the details of the organisation into the system, enters payment details and selects the profile for the organisation.

Once an organisation is created the system administrator can begin to load up the system and the essential on-boarding activities are:

1. Load of user details, including emails.
2. Assigning users to certain roles.
3. Review and confirmation of policies.
4. Inspection and confirmation of CSPM defaults for activities to be carried out as part of the regular Cyber Security protection activity.

Off boarding is straightforward. The organisation can choose to stop using the service by giving one month's notice. When off-boarding they can request that their data be extracted and provided in a standard file format. They then request a purge of the organisation's data from the system.

If an organisation stops paying for the service the access to all users, except the system administrator, will be suspended. After a further month, access for the system administrator will be suspended as well. In a further month the organisation will be deleted from the system.

Pricing

Base pricing is essentially £1 per user per calendar month. In addition, there will be a charge of £10 per calendar month for policies and £10 per calendar month for managers and administrators.

Further options are available on request.

There is a charge of £500 for data extraction and up to two hours of consultancy support to assist in the user understanding the data formats.

Service Management

The service is provided in two instances. The first is in the AWS California Region to service the US. The second is in the AWS London Region to service UK and EU customers.

Service provision is managed from our offices in Wimbledon, with limited follow the sun support from our staff based in Sacramento California.

Service tickets are submitted using the CSPM Service Desk instance available from the help page on the solution once a user has created an account. Users can email requests in or log in to the service desk portal where our support team will handle and respond to tickets.

Service Constraints

Releases are generally performed on a fortnightly basis though this may be more frequent.

Maintenance windows are typically about 2 hrs and are carried out outside working hours for the geography supported.

Details of changes in the release are provided.

Service Levels

The service is available 24 x 7 though we reserve the right to shut down the solution for updating and preventative maintenance giving reasonable notice in advance of planned maintenance.

Standard support hours are between 9 am to 5.30 pm during UK working days. Emergency cover is available for serious system outages at a reduced level 24 x 7.

Security

Every account is secured with username/email and password credentials which are encrypted at rest and in transit. The service is penetration tested; all vulnerabilities found that have a CVSS score of 4 and above are addressed as a top priority. We implement security features such as: session tokens, account lockout, service permissions, data encryption, access control lists and others to keep you and your data secure.

Financial Recompense Model

There is no provision for any financial recompense model for not meeting any specific service level.

Training

The objective is that the solution should be intuitive and require no specific training. To that end, a number of videos are provided to guide new users through the operation of the system and in addition help documents and text are provided that are context sensitive where appropriate to the information on the screen.

Ordering And Invoice Processing

Any organisation can go to the site, register and initiate a first invoice and a direct debit which will collect an initial payment for based on the number of users projected on the system.

Once the bank details have been entered into Xero (we hold no payment details) and the first payment has been received the system will be fully enabled for all users.

Invoicing is monthly in advance thereafter.

Termination Terms

A customer may terminate at any time giving one months' notice by selecting the leave system option in the system administrators screen. This function is only available to the current primary user.

Policy Monitor may terminate the G-cloud service giving 3 months' notice in the event that the Policy Monitor G-cloud contract for provision of this service is terminated. This notice shall be via email to the primary user and will be repeated by regular emails up to the point where the service is shutdown.

Data Restoration/Service Migration

Regular backups are taken (see above) and the restoration of data following a failure will be at least to the previous backup.

If data is deleted due to a customer operator error then it may be possible to recover this data from a backup but services to carry out such investigation shall be separately chargeable.

In the event of a service migration the user shall be able to export their data in a standard CSV format in a structure which could be reloaded into a database for transformation and re-load purposes. Policy Monitor responsibilities are limited to provision of the data.

The data available to be exported includes:

1. Details of staff
2. Hardware inventory
3. Software inventory
4. History of task execution
5. Customer loaded documents

Consumer Responsibilities

The customer's responsibilities are:

1. To operate the system in a manner based on good practice as defined in Cyber Essentials, particularly as regards use and protection of passwords.
2. To access the system only in approved and documented manners through the user interface or other published APIs made available.
3. To use the system in accordance with the system documentation. To task users in the activities that are designed to protect the organisation and to reduce the risk and impact of any attack.
4. To report any unexpected behaviours or concerns using the provided service desk Policy Monitor instance made accessible from application help pages.

Technical Requirements

CSPM is a browser-based system so the primary technical requirement is to access the system through an industry standard supported browser.

The front-end solution is based on HTML 5, CSS and java script and there should be no plugin mandated, though we reserve the right to require java support or similar for access to any remote services such as you tube or other services that might require it.

Our preferred browser is Chrome but Firefox, Edge, Safari and the latest versions of IE are all supported.

Our solution does not impose a heavy load on the network, but has areas where a number of separate calls are made so performance is optimised by a robust high bandwidth, low latency network in the customer's office.

Trial Service

Organisations will be awarded up to 1-month free access for one System Administrator to trial the service.

There is also a sandbox available that is exposed to the internet where users can set up demo accounts for training and experimentation purposes but no personal data or customer sensitive data is permitted on this demo system.